# **OFFENSIVE SECURITY**

# OSWP Exam Documentation

v.2.0

student@youremailaddress.com

OSID: XXXXX



Copyright © 2022 Offensive Security Ltd. All rights reserved.

No part of this publication, in whole or in part, may be reproduced, copied, transferred or any other right reserved to its copyright owner, including photocopying and all other copying, any transfer or transmission using any network or other means of communication, any broadcast for distant learning, in any form or by any means such as any information storage, transmission or retrieval system, without prior written permission from Offensive-Security.

Table of Contents

[1.0 Offensive-Security OSWP Exam Documentation 3](#__RefHeading___Toc54945904)

[2.0 Access Point X 4](#__RefHeading___Toc3008_3721744763)

[2.1 Wireless Network Key 4](#__RefHeading___Toc549459101)

[2.2 Screenshots 4](#__RefHeading___Toc2790_37217447631)

[2.3 Steps 4](#__RefHeading___Toc2790_372174476311)

[3.0 Access Point Y 5](#__RefHeading___Toc54945908)

[3.1 Proof 5](#__RefHeading___Toc54945909)

[3.2 Screenshots 5](#__RefHeading___Toc549459102)

[3.3 Steps 5](#__RefHeading___Toc2790_3721744763)

[4.0 Additional Items Not Mentioned in the Report 6](#__RefHeading___Toc3008_37217447631)

# 1.0 Offensive-Security OSWP Exam Documentation

The Offensive Security OSWP exam documentation contains all efforts that were conducted in order to pass the Offensive Security Wireless Professional exam. This report will be graded from a standpoint of correctness and fullness to all aspects of the exam. The purpose of this report is to ensure that the student has the technical knowledge required to pass the qualifications for the Offensive Security Wireless Professional certification.

You are required to fill out this exam documentation fully and to include the following sections:

* Methodology walkthrough and detailed outline of steps taken
* Each finding with included screenshots, walkthrough, and sample commands
* Any additional items that were not included

# 2.0 Access Point X

A brief description of the attack chain with machine names, including the depth of compromise should be included here.

## **2.1 Proof**

Provide the contents of the “Access Point X” wireless network key.

## **2.2 Screenshots**

Provide at least one screenshot of the successfully cracked “Access Point X" wireless network key and a screenshot of proof.txt.

## **2.3 Steps**

Provide a detailed account of your methodology in obtaining the “Access Point X” wireless network key. ***The steps taken should be able to be easily followed and reproducible if necessary***.

# 3.0 Access Point Y

While monitoring the wifi activity in the area, I discovered Access Point Y. Further enumeration I discovered that Access Point Y was transmitting on channel X and using XYZ as its security algorithm. I proceeded by collecting information by utilizing the XYZ attack, till there was enough information to crack the key using the 123 cracking tool.

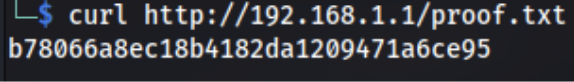
## **3.1 Proof**

The “Access Point 2” wireless network key: **DE:AD:CA:FE:BA:BE:99:77:55:33:11:88:66**

The “Access Point Y” proof.txt: **b78066a8ec18b4182da1209471a6ce95**

## **3.2 Screenshots**

*Cracked wireless key*

*Cracked wireless key*

## **3.3 Steps**

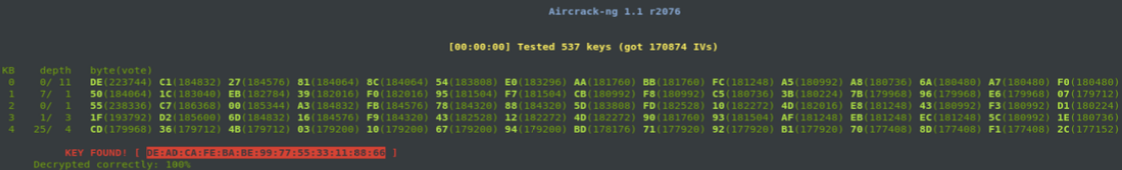
1. Placed interface in monitor mode.

*Command and/or screenshots*

2. Next Step

*Command and/or screenshots*

3. Crack the key using the 123 cracking tool.



# 4.0 Additional Items Not Mentioned in the Report

This section is placed for any additional items that were not mentioned in the overall report.